## DETAILED ACTION

1. This is in response to the amendment filed November 25, 2008. Claims 1 and 33 have been amended. Claims 1-5, 10, 11, 13-15, 33-37, 42 and 45-47 are pending and have been considered below.

## EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

3. Authorization for this examiner's amendment was given in a telephone interview with Vincent H. Anderson (Reg. No. 54,962) on March 12, 2009.

The application has been amended as follows:

Please amend claims 34-37, 42, 43 and 45-47as follows:

**34.** (**Currently Amended**) The ~~article~~ computer readable storage medium of claim 33, wherein a platform private key is bound to the platform configuration using the TPM.

**35.** (**Currently Amended**) The ~~article~~ computer readable storage medium of claim 34, wherein the TPM comprises a processor coupled to a protected storage device.

**36.** (**Currently Amended**) The ~~article~~ computer readable storage medium of claim 33, wherein instructions for cryptographically hashing the platform configuration comprises instructions for cryptographically hashing the platform configuration using a secure hashing algorithm.

**37.** (**Currently Amended**) The ~~article~~ computer readable storage medium of claim 36, wherein the secure hashing algorithm comprises Secure Hashing Algorithm Version 1.0 (SHA-1).

**42.** (**Currently Amended**) The ~~article~~ computer readable storage medium of claim 33, wherein the platform configuration includes multiple identities and the platform key includes one or more platform identity keys.

**43.** (**Canceled**)

**45.** (**Currently Amended**) The ~~article~~ computer readable storage medium of claim 33, further comprising instructions for:

exchanging an explanation of the platform configuration hashes following session key negotiations to finalize the authentication;

verifying, at both endpoints, key exchange messages, certificates and platform configuration data; and

authenticating the session if no problems arise during verification.

**46.** (**Currently Amended**) The ~~article~~ computer readable storage medium of claim 45, further comprising instructions for halting the authentication session if problems arise during verification.

**47.** (**Currently Amended**) The ~~article~~ computer readable storage medium of claim 45, further comprising instructions for enabling endpoints to exchange data, wherein each endpoint knows that the platform from the other endpoint has been authenticated using a platform identity that ties to the trusted platform module.

***Allowance***

5. Claims 1 and 33 have been amended with written arguments, which overcome the examiner's prior rejection see argument of 11/25/2008. Examiner withdraws all outstanding rejections

Claims 1-5, 10, 11, 13-15, 33-37, 42 and 45-47 are allowed.

***Examiner's Statement of Reason for allowance***

6. The following is an examiner's statement of reasons for allowance:

7. Uusitalo et al (US 2005/0063544) discloses a method of facilitating the lawful interception of an IP session between two or more terminals wherein said session uses encryption to secure traffic. Prior to the creation of the session, a seed value is exchanged between the terminals at which the key is stored and the node. The key and the seed value are used at both the terminal and the node to generate a pre-master key. The pre-master key becomes known to each of the terminals involved in the IP session and to the network node. The pre-master key is used, directly or indirectly, to encrypt and decrypt traffic associated with said IP session

8. Wiseman et al (US 7,216,369) discloses a system which include a root of trust for measurement (RTM) module coupled to a verified platform security property policy module and a comparison module. The comparison module may operate to prevent transfer of control to an operating system (and/or halt the boot process) if a policy included in the platform security property policy module is violated.

9. Bass et al (US 4,649,233) discloses a method for authenticating nodes/users and in protecting data flow between nodes. The method is facilitated by creating a dialogue involving authenticated encryption among the nodes. During each session, a key for use in cryptographic conversion is constructed among the node participants in order to permit symmetric authentication. The key is unique to the session. A different key is generated for each and every session.

10. The prior art of record taken alone or in combination do not teach or render obvious the limitations as recited in independent claims 1 and 33. The cited references, whether alone or in combination fail to disclose or suggest the following limitation:

1. a pre-master secret from which a master secret is derived;
2. signing a master secret with multiple authentication facets, or a master secret signed with multiple authentication keys; and
3. late binding of the secure channel to prevent the binding from persisting outside the secure channel

11. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance.

***Conclusion***

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FATOUMATA TRAORE whose telephone number is

(571)270-1685. The examiner can normally be reached on Monday- Friday (every other Friday off) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Friday March 13, 2009

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436